Information om to-faktor-login, cookies og RPA i DUBU

Indhold

Krav om to-faktor-login ved skift til Context Handler 2

Den nye version af Fælleskommunal Adgangsstyring for brugere, Context Handler 2, håndhæver to-faktor autentifikation, når brugere logger på it-systemer, der kræver sikringsniveauerne NIST 3 og 4, samt NSIS ”Betydelig” og ”Høj”.

To-faktor autentifikation betyder, at en bruger skal bekræfte sin identitet med to individuelle faktorer ved login. De to faktorer skal være forskellige og kan fx være:

- Brugernavn og kodeord (noget du ved)
- Biometri, fx ansigtsgenkendelse (noget du er)
- Autentifikations-app på din telefon (noget du har)

Log-in vil som regel forgå i to trin, hvor brugeren fx først taster sit brugernavn og adgangskode, og derefter modtager en engangskode via en app på telefonen.

DUBU kræver sikringsniveau NIST 3. Brugere af DUBU skal derfor være tildelt to-faktor autentifikation for at kunne logge på, når DUBU skifter til Context Handler 2 d. 28. februar 2025.

Det er den enkelte kommune, der tildeler to-faktor autentifikation til sine brugere. Inden DUBU skifter til Context Handler 2, publicerer KOMBIT derfor en KLIK-opgave til din kommunes DUBU-systemansvarlige om tildeling af to-faktor autentifikation til evt. brugere, der mangler det.

Kommunens brugere logger på DUBU via kommunens Identity Provider (IdP). Nogle kommuner kan have valgt en opsætning for deres IdP, (”*Without requested LoA*”), der betyder, at kommunen selv har ansvar for, at brugere altid er logget på med to-faktor autentifikation (eller tilsvarende) til de it-systemer, der kræver det. Hvis en kommune har valgt det, vil kommunens brugere ikke nødvendigvis opleve at blive bedt om to-faktor-login, hvis de logger på via den IdP, fordi kommunen har sikret styrken af brugerens autentifikation på anden vis.

Du kan læse mere om Context Handler 2 i Digitaliseringskataloget.

Min kommune har forskellige IdP'er – hvad betyder det for brugere ved login via Context Handler 2?

Flere kommuner har mere end en Identity Provider (IdP) og nogle af disse kommuner har derfor valgt at tilslutte flere IdP'er til Context Handler 2.

Hvis det er tilfældet i din kommune, kan det være, at jeres brugere skal vælge en anden IdP, når de skal logge ind via Context Handler 2, end den de tidligere har brugt. Din kommunes it-afdeling vil kunne oplyse, om det er noget, jeres brugere skal være opmærksomme på.

Cookies i browser
Hvis en bruger har sat hak i "*Husk mit valg*" ved et tidligere login via Fælleskommunal Adgangsstyring for brugere, ligger der en cookie i brugerens browser. Browseren "husker" derfor hvilken IdP, brugeren valgte ved login.

På grund af cookien, vil browseren forsøge at kontakte den samme IdP næste gang, brugeren logger på via Fælleskommunal Adgangsstyring for brugere.

Hvis den IdP, som browseren husker, *ikke* er den IdP, som brugeren skal bruge til at logge på via Context Handler 2, vil brugeren opleve en fejl ved forsøg på login via Context Handler 2. Brugeren (eller din kommunes it-afdeling) skal derfor fjerne cookien, så brugeren kan vælge den rigtige IdP.

Softwarerobotter (RPA) og Context Handler 2

Softwarerobotter (RPA) er for nuværende kun understøttet med NIST-sikringsniveauer. Det betyder, at RPA-brugere kun må logge på et it-system via Context Handler 2, hvis it-systemet kræver et NIST-sikringsniveau.

En RPA-bruger må til gengæld *ikke* logge på et it-system, der kræver et NSIS-sikringsniveau. Det skyldes, at selve NSIS-standarden p.t. kun understøtter fysiske personer og juridiske enheder. KL og KOMBIT afventer en afklaring fra Digitaliseringsstyrelsen på, hvordan dette skal løses.

Du kan læse mere om hvordan en kommune kan lade softwarerobotter logge på it-systemer med NIST-sikringsniveauer via Context Handler 2 i denne nyhed i Digitaliseringskataloget.